

PLA



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/674,950	01/10/2001	Angel Jose Ferre Herrero	932.1173	8745

21831 7590 08/25/2004

STEINBERG & RASKIN, P.C.  
1140 AVENUE OF THE AMERICAS, 15th FLOOR  
NEW YORK, NY 10036-5803

EXAMINER
----------

ADAMS, JONATHAN R

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/674,950	FERRE HERRERO, ANGEL JOSE	
	<b>Examiner</b>	<b>Art Unit</b>	
	Jonathan R Adams	2134	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 10 January 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☐ Claim(s) \_\_\_\_\_ is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 and 18-40 is/are rejected.
- 7) ☒ Claim(s) 14-17 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-9, 18-20, 23-30, 35-40 rejected under 35 U.S.C. 102(b) as being anticipated by Alfred Menezes et al., "Handbook of Applied Cryptography".

As to claim(s) 1-4, 23-26:

3. Menezes teaches a data sequence encryption system using a selectable control block for use in IDEA encryption in CBC mode comprising:

- Receiving a plaintext sequence / Assemble plaintext sequence in plurality of plaintext blocks size N / Partition the message into n-bit blocks and encrypt each separately (Page 228, Line 10, Menezes)
- Receiving a control block / Input: k-bit key (Page 228, Line 5, Menezes)
- Divide control block into a control initial block of length g and a control initial block of length 2N / IDEA algorithm Input: 64-bit plaintext; 128-bit key (Page 264, Line 1, Menezes), CBC Input: ... n-bit Initialization vector, n-bit plaintext blocks

Art Unit: 2134

- Generate a plurality of transformer blocks with control initial block and randomized-encrypted text blocks / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)
- Generate encryption control subblocks with control initial block size  $2N$  / Compute 16-bit subkeys (Page 264, Line 3, Menezes)
- Generate grouped inter-blocks with plaintext block and corresponding transformer block / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)
- Generate randomized-encrypted text blocks with inter-blocks and encryption control subblocks / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)
- Output encrypted text block as encrypted text sequence / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)
- Randomized text sequence corresponds to plaintext sequence / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)

4. As to claim(s) 5, 27, 35-40:

Transformer block generating means implementing a function  $H$  / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1}(XOR)X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)

Art Unit: 2134

5. As to claim(s) 6, 28:

Grouping means include an XOR operation / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1} \oplus X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)

6. As to claim(s) 7, 18:

Transformer block equal to nth block of length N generated by  $E_n = \text{control initial block XOR nth minus one encrypted text block}$  / Encryption:  $C_0 \leftarrow IV$ ;  $C_j \leftarrow EK(C_{j-1} \oplus X_j)$  (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)

7. As to claim(s) 8, 19, 29:

Transformer block generating means implement function  $E_n$  as  $E_n(R_i) = (E_{n-1}(R_i) \oplus B) \bmod 2^{(Q_i)}$ , wherein  $Q_i$  is less than or equal to 64... / When  $Q_i = N = 64$  and  $B = 0$ , function  $E(n) = E(n-1)$  which could equal  $C_{(j-1)}$  as in (Page 230, Line 7, Menezes), (Page 229, Fig 7.1(b), Menezes)

8. As to claim(s) 9, 20, 30:

Control initial block of length  $2N$  made up of 128 bits and Control initial block of length  $G$  made up of 64 bits / IDEA algorithm Input: 64-bit plaintext; 128-bit key (Page 264, Line 1, Menezes), CBC Input: ... n-bit Initialization vector, n-bit plaintext blocks (Page 230, Line 5, Menezes)

Art Unit: 2134

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 10, 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Bruce Schneier, "Applied Cryptography".

Menezes teaches a data sequence encryption system using a selectable control block for use in IDEA encryption in CBC mode using a transformer block generating means and initialization vector. Menezes does not teach for the initialization vector to be generated randomly in the CBC mode section. Schneier teaches using randomly generated initialization vectors for use with block ciphers in CBC mode (Page 194, Line 8, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to generator a random number for use with the initialization vector as taught by Schneier. One of ordinary skill in the art would have been motivated to generator a random number for use with the initialization vector as taught by Schneier to increase the level of security for messages with standard headers .

11. Claims 11-13, 21, 22, 32, and 33 rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Schneier in further view of Jakubowski et al., US Patent No 6128737 (hereafter referred to as '737).

Art Unit: 2134

Menezes as modified above teaches a data sequence encryption system using a selectable control block for use in IDEA encryption in CBC mode using a transformer block generating means and randomly generated initialization vector. Menezes as modified above does not teach for the function En to include a hash function or for control initial block to be made up of seed length of random number generator. '737 teaches a CBC MAC encryption system using hashed bits from a transformer block generator of a given length for an encryption seed (Fig 4a, Elements 422, 423, 445, '737) (Col 4, Line 11, '737). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the hashed bits from a transformer block as the encryption seed as in '737 with the invention of Menezes as modified above. One of ordinary skill in the art would have been motivated to use the hashed bits from a transformer block as the encryption seed as in '737 with the invention of Menezes as modified above because seeds for random number generation need to themselves be random and hash functions provide an easy method for providing random numbers.

12. As to claim(s) 13, 22, 34:

Control initial block 2N made up of 128 bits and control initial block G made up of zero or more bits / IDEA algorithm Input: 64-bit plaintext; 128-bit key (Page 264, Line 1, Menezes), CBC Input: ... n-bit Initialization vector, n-bit plaintext blocks (Page 230, Line 5, Menezes)

Art Unit: 2134

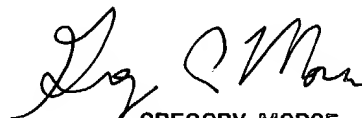
***Allowable Subject Matter***

13. Claims 14-17 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

15. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100